

ANNALES DE L'INSTITUT FOURIER

NICOLE MOSER

Sur les unités d'une extension galoisienne non abélienne de degré pq du corps des rationnels p et q nombres premiers impairs

Annales de l'institut Fourier, tome 29, n° 1 (1979), p. 137-158

http://www.numdam.org/item?id=AIF_1979__29_1_137_0

© Annales de l'institut Fourier, 1979, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

SUR LES UNITÉS
D'UNE EXTENSION GALOISIENNE NON ABÉLIENNE
DE DEGRÉ pq DU CORPS DES RATIONNELS,
 p ET q NOMBRES PREMIERS IMPAIRS

par **Nicole MOSER**

Dédié à Monsieur Claude Chabauty.

Le but de cet article est l'étude de la structure, en tant que module sur l'algèbre du groupe de Galois, du groupe des unités U_K d'une extension galoisienne K/\mathbf{Q} non abélienne de degré pq . La connaissance de cette structure est en effet précieuse pour déterminer de nombreuses propriétés arithmétiques de K : les indices des groupes de normes d'unités sur les corps intermédiaires, la participation de p au nombre de classes d'idéaux de K , des conditions nécessaires d'existence d'une unité de Minkowski. . .

Le premier paragraphe sert à dresser une liste de $\mathbf{Z}[G]$ -modules de référence, pour G groupe non abélien d'ordre pq . Les résultats figurent déjà dans un article de Lena Chang Pu [10] ; mais on reprend une partie des démonstrations d'un point de vue cohomologique, afin de poursuivre plus aisément les calculs.

On étudie ensuite différents invariants arithmétiques qui permettent d'obtenir les propriétés annoncées. Dans le cas particulier où les corps cyclotomiques $\mathbf{Q}^{(p)}$ et $\mathbf{Q}^{(q)}$ sont principaux, et où q^2 ne divise pas $p-1$, ces invariants caractérisent les différentes structures de $\mathbf{Z}[G]$ -module considérées. De plus, en interprétant les groupes de cohomologie relatifs à U_K comme le fait K. Iwasawa (cf. [7]), en termes d'idéaux ou de classes d'idéaux de K , on obtient quelques renseignements sur les homomorphismes d'extension des idéaux, et sur les idéaux premiers ramifiés. Enfin, on donne une illustration numérique, grâce à la théorie du corps de classes.

NOTATIONS

Pour tout corps de nombres totalement réel Λ , nous notons U_Λ le groupe des unités, et E_Λ le quotient $U_\Lambda/\{\pm 1\}$. Si Λ' est une sous-extension de Λ/\mathbf{Q} , l'application norme $N_{\Lambda/\Lambda'} : U_\Lambda \longrightarrow U_{\Lambda'}$ définit par passage aux quotients une application de E_Λ dans $E_{\Lambda'}$, notée encore $N_{\Lambda/\Lambda'}$.

Le lettre G désigne un groupe métacyclique d'ordre pq , (p et q sont deux nombres premiers impairs tels que q divise $p-1$), engendré par deux éléments σ et τ liés par les relations :

$$\sigma^p = \tau^q = 1$$

$$\tau\sigma = \sigma^r\tau,$$

où r est une racine primitive q -ième de l'unité modulo p . Nous réservons la lettre K pour désigner une extension galoisienne de \mathbf{Q} , de groupe G ; nous notons k le sous-corps de K fixe par H , groupe cyclique engendré par σ , et L le sous-corps qui correspond à g , sous-groupe de G engendré par τ .

Enfin, les lettres p et q ayant la signification donnée ci-dessus, nous notons :

ζ une racine primitive p -ième de l'unité ;

$\mathbf{Q}^{(p)}$ le p -ième corps cyclotomique ;

$A = \mathbf{Z}[\zeta]$ et $\mathfrak{A} = (1 - \zeta)A$;

ψ l'élément d'ordre q du groupe cyclique $\text{Gal}(\mathbf{Q}^{(p)}/\mathbf{Q})$, défini par $\zeta \longmapsto \zeta^r$;

\mathbf{Q}_1 le sous-corps de $\mathbf{Q}^{(p)}$ fixe par ψ ;

$A_1 = \mathbf{Q}_1 \cap A$ et $\mathfrak{A}_1 = A_1 \cap \mathfrak{A}$;

h_1 le nombre de classes d'idéaux de A_1 ;

θ une racine primitive q -ième de l'unité ;

$B = \mathbf{Z}[\theta]$;

h_q le nombre de classes d'idéaux de B .

De plus, φ désigne la fonction d'Euler.

1. STRUCTURE DE G-MODULE DE E_K

Si, pour tout sous-groupe Δ de G , on note χ_Δ^* le caractère de G induit par le caractère unité χ_Δ de Δ , on sait que le groupe E_K est un G -module de caractère $\chi_{\{1\}}^* - \chi_G$. Dans ce paragraphe, on construit une liste de G -modules telle que tout module de caractère $\chi_{\{1\}}^* - \chi_G$ soit isomorphe à un des termes de la liste au moins.

Soit R un G -module de caractère $\chi_{\{1\}}^* - \chi_G$, sans \mathbf{Z} -torsion ; la méthode utilisée pour étudier sa structure est due à I. Reiner : elle consiste à considérer R comme une extension d'un $\mathbf{Z}[g]$ -module R_0 par un module \tilde{R} annulé par $(1 + \sigma + \dots + \sigma^{p-1})$.

1.1. Définition et structure de \tilde{R} .

Supposons R noté additivement, et posons

$$\tilde{R} = \{x \in R \mid (1 + \sigma + \dots + \sigma^{p-1})x = 0\}.$$

Puisque R est de caractère $\chi_{\{1\}}^* - \chi_G$, le \mathbf{Z} -rang de \tilde{R} est égal à $(p - 1)q$. Ainsi, \tilde{R} est un $\mathbf{Z}[G]/(1 + \sigma + \dots + \sigma^{p-1}) \mathbf{Z}[G]$ -module, sans \mathbf{Z} -torsion, de \mathbf{Z} -rang $(p - 1)q$: sa structure est connue grâce aux travaux de M. Rosen ([15]), et l'on peut énoncer :

PROPOSITION 1.1. — \tilde{R} est $\mathbf{Z}[G]$ -isomorphe à la somme directe de q idéaux invariants de A/A_1 : $\tilde{R} \simeq \bigoplus_{i=1}^q \mathfrak{P}^{e_i} \alpha_i$, les α_i appartenant à un système de représentants des classes de A_1 , et les e_i étant compris entre 0 et $q - 1$. De plus, \tilde{R} est défini, à isomorphisme près, par les e_i et la classe de $\prod_{i=1}^q \alpha_i$.

Rappelons que σ agit sur chaque $\mathfrak{P}^{e_i} \alpha_i$ par multiplication par ζ , et que τ opère comme l'application ψ .

1.2. Définition et structure de R_0 .

Notons R_0 le quotient R/\tilde{R} ; c'est un module de \mathbf{Z} -rang $(q - 1)$, et par définition de \tilde{R} , il est invariant par σ . Sa structure

en tant que $\mathbf{Z}[G]$ -module est entièrement définie par sa structure en tant que $\mathbf{Z}[g]$ -module. D'après les hypothèses sur le caractère de R , aucun élément non trivial de R_0 n'est fixe par τ . On utilise alors les résultats de I. Reiner ([14]) sur les représentations entières d'un groupe cyclique d'ordre premier. Pour le module R_0 , il n'y a qu'une possibilité :

PROPOSITION 1.2. — R_0 est $\mathbf{Z}[G]$ -isomorphe à un idéal \mathfrak{b} de B . Sur cet idéal, σ opère trivialement, tandis que τ agit par multiplication par θ .

1.3. Extensions de R_0 par \tilde{R} .

On démontre (voir par exemple [16]) que l'existence d'extensions indécomposables de R_0 par \tilde{R} équivaut à l'existence d'éléments non nuls dans $H^1(G, \text{Hom}_{\mathbf{Z}}(R_0, \tilde{R}))$, et que les groupes $H^1(G, \text{Hom}_{\mathbf{Z}}(\mathfrak{b}, \mathfrak{P}^e \alpha))$ et $H^1(G, \text{Hom}_{\mathbf{S}}(S[\theta], (1 - \zeta)^e S))$ sont isomorphes ; (S désigne l'intersection des localisés $\mathbf{Z}_{(p)}$ et $\mathbf{Z}_{(q)}$).

PROPOSITION 1.3. — Le groupe $H^1(G, \text{Hom}_{\mathbf{S}}(S[\theta], (1 - \zeta)^e S))$ est trivial si $e = 1$; sinon il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Démonstration. — Le module $S[\theta]$ est S -libre, de base $\{1, \theta, \dots, \theta^{q-2}\}$, donc $\text{Hom}_{\mathbf{S}}(S[\theta], (1 - \zeta)^e S)$ est isomorphe, en tant que S -module, à $((1 - \zeta)^e S)^{q-1}$. Posons $M = ((1 - \zeta)^e S)^{q-1}$, et munissons M de la structure de G -module induite par celle de $\text{Hom}_{\mathbf{S}}(S[\theta], (1 - \zeta)^e S)$: σ opère sur M par multiplication par ζ , et pour tout $(a_0, a_1, \dots, a_{q-2})$ de M ,

$$\tau(a_0, a_1, \dots, a_{q-2}) = \left(- \sum_{i=0}^{q-2} \psi(a_i), \psi(a_0), \dots, \psi(a_{q-3}) \right).$$

Comme le sous-module de M fixe par σ est trivial, l'application restriction est un isomorphisme entre les groupes $H^1(G, M)$ et $H^1(H, M)^{G/H}$. Considérons donc un élément c de $Z^1(H, M)$; il est défini par l'image $u \in M$ qu'il donne de σ , et le transformé de c par τ associe à l'élément σ l'élément $\tau^{-1}[(1 + \zeta + \dots + \zeta^{r-1})u]$. La condition "c représente une classe fixe par τ " s'exprime par l'existence d'un élément $v \in M$ tel que :

$$\tau^{-1} [(1 + \zeta + \dots + \zeta^{r-1})u] - u = (1 - \zeta)v.$$

Si $u = (u_0, u_1, \dots, u_{q-2})$, chaque u_i s'écrit $(\zeta - 1)^e x_i$, $x_i \in S[\zeta]$. Notons \bar{x}_i la classe de x_i modulo $(\zeta - 1)S[\zeta]$. On obtient le système dans $S[\zeta]/(\zeta - 1)S[\zeta]$:

$$\left\{ \begin{array}{l} r\bar{x}_0 + r^e \sum_{i=0}^{q-2} \bar{x}_i = 0 \\ r\bar{x}_1 - r^e \bar{x}_0 = 0 \\ \vdots \\ r\bar{x}_{q-2} - r^e \bar{x}_{q-3} = 0. \end{array} \right.$$

Comme r est inversible modulo p , les $q - 2$ dernières équations du système donnent, pour $1 \leq i \leq q - 2$: $\bar{x}_i = r^{i(e-1)} \bar{x}_0$. En reportant ces valeurs dans la première équation, on obtient :

$$\bar{x}_0 \left(\sum_{i=0}^{q-1} r^{i(e-1)} \right) = 0.$$

Si $e = 1$, $\sum_{i=0}^{q-1} r^{i(e-1)} = q$, donc $\bar{x}_0 = 0$, et le groupe de cohomologie étudié est trivial. Sinon, \bar{x}_0 peut être choisi arbitrairement dans $S[\zeta]/(1 - \zeta)S[\zeta]$, et le groupe de cohomologie est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. ■

PROPOSITION 1.4. — On note U^* l'image du groupe des unités de A_1 par l'homomorphisme canonique de A sur A/\mathfrak{P} , \bar{r} l'image de r dans $\mathbf{Z}/p\mathbf{Z}$, et V^* l'image du groupe des unités de $S[\theta]$ par le S -homomorphisme de $S[\theta]$ dans $\mathbf{Z}/p\mathbf{Z}$ défini par $\theta^i \mapsto r^{i(e-1)}$. Si $\langle U^*, V^* \rangle$ est le sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^*$ engendré par U^* et V^* , le nombre d'extensions indécomposables deux à deux non $S[G]$ -isomorphes de $S[\theta]$ par \mathfrak{P}^e ($e \neq 1$) est égal à l'indice $[(\mathbf{Z}/p\mathbf{Z})^* : \langle U^*, V^* \rangle]$.

Démonstration. — Elle utilise le théorème suivant de I. Reiner ([16]).

THEOREME. — Soit G un groupe fini d'ordre ℓ , I l'ensemble des diviseurs premiers de ℓ , et S l'intersection des localisés de \mathbf{Z} en s lorsque s parcourt I . Soit M_0 et M_1 deux $S[G]$ -modules irréductibles non isomorphes, et f et g deux éléments de

$Z^1(G, \text{Hom}_S(M_0, M_1))$. Les extensions (M_1, M_0, f) et (M_1, M_0, g) sont $S[G]$ -isomorphes si et seulement si l'on peut trouver un $S[G]$ -automorphisme α de M_1 , un $S[G]$ -automorphisme β de M_0 , et $c \in \text{Hom}_S(M_0, M_1)$ tels que pour tout $m \in M_0$ et tout $x \in G$, on ait :

$$\alpha f_x(xm) - g_x(x\beta m) = xc(m) - c(xm). \quad (1)$$

On applique ce résultat pour $M_1 = \mathfrak{P}^e$ et $M_0 = S[\theta]$. Si f et g définissent des extensions isomorphes, on pose $f^* = \alpha f$ et $g^* = g\beta$: les quatre extensions de $S[\theta]$ par \mathfrak{P}^e définies respectivement par f, f^*, g et g^* sont $S[G]$ -isomorphes.

D'après les calculs de la proposition 1.3, les cocycles sont caractérisés par la valeur de leur image de σ en 1, premier élément de la base canonique de $S[\theta]$. L'élément σ agit trivialement sur $S[\theta]$; on déduit donc de (1) que f^* et g^* ont même image dans $(Z/pZ)^*$.

Comme \mathfrak{P}^e est un S -module libre de base

$$\{(1 - \zeta)^e, (1 - \zeta)^e \zeta, \dots, (1 - \zeta)^e \zeta^{p-2}\},$$

il est clair que tout automorphisme de \mathfrak{P}^e compatible avec l'action de σ opère comme la multiplication par une unité de A . Si de plus cet automorphisme commute avec τ , l'unité doit appartenir à A_1 ; donc f et f^* ont des images dans $(Z/pZ)^*$ congrues modulo U^* .

De manière analogue, on vérifie que l'automorphisme β est en fait la multiplication par une unité ϵ de $S[\theta]$. Posons $\epsilon = \sum_{i=0}^{q-2} \lambda_i \theta^i$. Alors $g_\sigma \beta(1_{S[\theta]}) = g_\sigma \left(\sum_{i=0}^{q-2} \lambda_i \theta^i \right) = \sum_{i=0}^{q-2} \lambda_i r^{i(e-1)} g_\sigma(1)$, et g et g^* ont des images congrues modulo V^* . Donc f et g ont des images congrues modulo $\langle U^*, V^* \rangle$.

La réciproque s'obtient simplement en remontant les calculs et en utilisant la réciproque du théorème de I. Reiner. ■

LEMME 1.5. — L'indice $[(Z/pZ)^* : \langle U^*, V^* \rangle]$ vaut 1 ou q . Si p n'est pas congru à 1 modulo q^2 , il est égal à 1.

Démonstration. — Galovitch, Reiner et Ullom ont calculé dans [4] l'indice $[(Z/pZ)^* : U^*]$: il vaut q , donc $[(Z/pZ)^* : \langle U^*, V^* \rangle]$ divise q .

Le groupe V^* contient l'image \bar{r}^{e-1} de θ , qui est un élément de $(\mathbf{Z}/p\mathbf{Z})^*$ d'ordre q . Comme $\text{Card } U^* = \frac{p-1}{q}$, si p n'est pas congru à 1 modulo q^2 , \bar{r}^{e-1} n'appartient pas à U^* , et $\langle U^*, V^* \rangle = (\mathbf{Z}/p\mathbf{Z})^*$. ■

LEMME 1.6. — Soit $\left(\bigoplus_{i=1}^q \mathfrak{P}^{e_i}, S[\theta]\right)$ une extension construite à l'aide de cocycles f_i non triviaux. S'il existe deux indices j et k tels que $e_j = e_k$, et que f_j soit équivalent à f_k modulo un cobord, alors $\left(\bigoplus_{i=1}^q \mathfrak{P}^{e_i}, S[\theta]\right)$ est $S[G]$ -isomorphe à $\left(\bigoplus_{\substack{i=1 \\ i \neq j}}^q \mathfrak{P}^{e_i}, S[\theta]\right) \oplus \mathfrak{P}^{e_j}$.

Démonstration. — Pour faciliter la rédaction, choisissons $j = 1$ et $k = 2$. Posons $M = \left(\bigoplus_{i=1}^q \mathfrak{P}^{e_i}, S[\theta], f_i\right)$ et

$$M' = \mathfrak{P}^{e_1} \oplus \left(\bigoplus_{i=2}^q \mathfrak{P}^{e_i}, S[\theta], 2f_2, f_3, \dots, f_q\right).$$

Il est clair que l'application Φ de M dans M' définie par :

$$(a_1, a_2, \dots, a_q, b) \longmapsto (a_1 - a_2, a_1 + a_2, a_3, \dots, a_q, b),$$

avec $a_i \in \mathfrak{P}^{e_i}$ et $b \in S[\theta]$, est une bijection S -linéaire. De plus, on a :

$$\Phi\sigma(a_1, a_2, \dots, a_q, b) = \sigma\Phi(a_1, \dots, a_q, b)$$

et
$$\Phi\tau(a_1, a_2, \dots, a_q, b) = \tau\Phi(a_1, \dots, a_q, b).$$

Donc les $S[G]$ -modules M et M' sont isomorphes. ■

1.4. Conclusion.

Tout $\mathbf{Z}[G]$ -module de caractère $\chi_{\{1\}}^* - \chi_G$ est isomorphe à l'un au moins des modules de la liste suivante :

- $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j \oplus \mathfrak{b}$
- $\left(\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b}\right) \bigoplus_{j=l+1}^q \mathfrak{P}^{e_j} \alpha_j.$

Rappelons que \mathfrak{b} désigne un idéal de B , que tous les e_j vérifient la condition $0 \leq e_j \leq q - 1$, et que les α_j sont choisis dans un système exact de représentants des classes d'idéaux de A_1 .

De plus, $\left(\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b}\right)$ désigne une extension de \mathfrak{b} par $\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \alpha_j$, construite à l'aide de cocycles non triviaux ; (cela entraîne en particulier que pour $1 \leq j \leq \ell$, les e_j sont distincts de 1). D'après le lemme 1.6, on peut aussi imposer que si $e_j = e_k$, j et k appartenant à l'intervalle $[1, \ell]$, les cocycles correspondants ne soient pas cohomologues.

2. CONSEQUENCES ARITHMETIQUES DE LA STRUCTURE DE G-MODULE DE E_K

2.1. Etude de l'application $N_{K/L} : E_K \longrightarrow E_L$.

PROPOSITION 2.1. — *Le groupe E_L s'identifie au sous-groupe de E_K formé des éléments fixes par τ . Si \tilde{E}_K est isomorphe à $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$, E_L est isomorphe à $\bigoplus_{j=1}^q \mathfrak{P}_1^{\tilde{e}_j} \alpha_j$; \tilde{e}_j est un entier qui vaut 0 si $e_j = 0$, et 1 sinon. De plus, l'application $N_{K/L} : \tilde{E}_K \longrightarrow E_L$ est surjective.*

Démonstration. — Il est clair que tout élément de E_L est fixe par τ . Inversement, soit u un élément de E_K fixe par τ ; il est représenté par un élément ϵ de U_K ; si $\epsilon^\tau = -\epsilon$, ϵ serait fixe par τ^2 , ce qui conduit à une contradiction; donc $\epsilon^\tau = \epsilon$, et $u \in E_L$.

D'après le paragraphe 1.1, le sous-module \tilde{E}_K de E_K annihilé par $(1 + \sigma + \dots + \sigma^{p-1})$ est isomorphe à une somme directe $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$. Comme E_L est inclus dans \tilde{E}_K , E_L est isomorphe au sous-groupe de $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$ fixe par τ , c'est-à-dire à $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j \cap A_1 = \bigoplus_{j=1}^q \mathfrak{P}_1^{\tilde{e}_j} \alpha_j$.

A l'élément ξ de \tilde{E}_K est associé l'élément $(\alpha_1, \dots, \alpha_q)$ de $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$, et à $N_{K/L}(\xi)$ correspond $(\text{Tr}_{\mathbf{Q}^{(p)}/\mathbf{Q}_1}(\alpha_1), \dots, \text{Tr}_{\mathbf{Q}^{(p)}/\mathbf{Q}_1}(\alpha_q))$. L'extension $\mathbf{Q}^{(p)}/\mathbf{Q}_1$, de degré q , est modérément ramifiée, donc

l'application $\text{Tr}_{\alpha^{(p)}/\alpha_1}$ est une surjection de A sur A_1 . Cela prouve que l'application $N_{K/L} : E_K \rightarrow E_L$ est une surjection de \tilde{E}_K sur E_L . ■

Remarque. — Une démonstration de la surjectivité de l'application $N_{K/L} : E_K \rightarrow E_L$ figure déjà dans un article de C.D. Walter [17].

2.2. Etude de l'application $N_{K/k} : E_K \rightarrow E_k$.

PROPOSITION 2.2. — *Le groupe E_k s'identifie au sous-groupe de E_K formé des éléments fixes par σ . Si E_K est isomorphe à $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j \oplus \mathfrak{b}$, E_k est isomorphe à \mathfrak{b} . Si E_K est isomorphe à $\left(\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b} \right) \bigoplus_{j=\ell+1}^q \mathfrak{P}^{e_j} \alpha_j$, E_k est isomorphe à $\mathfrak{p}_q^{(1)} \dots \mathfrak{p}_q^{(u)} \mathfrak{b}$; les $\mathfrak{p}_q^{(i)}$ sont des idéaux premiers de B au-dessus de p , deux à deux distincts, et l'entier u est égal au nombre d'exposants e_j distincts, pour $1 \leq j \leq \ell$.*

Démonstration. — L'identification de E_k au sous-groupe de E_K formé des éléments fixes par σ s'obtient comme celle de E_L à un sous-groupe de E_K .

Il est clair que le sous-groupe de $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j \oplus \mathfrak{b}$, fixe par σ , est \mathfrak{b} . D'autre part, les modules $\left(\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b} \right)$, $\bigoplus_{j=\ell+1}^q \mathfrak{P}^{e_j} \alpha_j$ et $M = \left(\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b} \right)$ admettent le même sous-groupe fixe par σ ; remarquons que ce sous-groupe s'identifie à $H^0(H, M)$. Si $Z_{(p)}$ désigne le localisé de Z en p , il est bien connu que les groupes $Z_{(p)} \otimes_Z H^0(H, M)$ et $H^0(H, Z_{(p)} \otimes_Z M)$ sont isomorphes. Le module $M_{(p)} = Z_{(p)} \otimes_Z M$ est une extension de $Z_{(p)}[\theta]$ par $\bigoplus_{j=1}^q \mathfrak{P}^{e_j}$, définie à l'aide de cocycles $f_j \in Z^1(G, \text{Hom}_{Z_{(p)}}(Z_{(p)}[\theta], \mathfrak{P}^{e_j}))$ non triviaux. Par des calculs analogues à ceux de la proposition 1.3, on vérifie que chaque f_j est déterminé par $(f_j)_\sigma(1) = (1 - \zeta)^{e_j} \epsilon_j$, $\epsilon_j \notin \mathfrak{P}$.

Désignons par (a_1, \dots, a_ℓ, b) un élément de $M_{(p)} : a_i \in \mathfrak{P}^{e_i}$ et $b \in Z_{(p)}[\theta]$. Cet élément est fixe par σ si et seulement si, pour

pour tout indice $j \in [1, \ell]$, on a : $(f_j)_\sigma(b) = (1 - \xi)a_j$. Or b s'écrit $x_0 + x_1\theta + \dots + x_{q-2}\theta^{q-2}$, $x_i \in \mathbf{Z}_{(p)}$, et

$$(f_j)_\sigma(b) = (1 - \xi)^{e_j} \epsilon_j \times (x_0 + x_1 r^{e_j-1} + \dots + x_{q-2} (r^{e_j-1})^{q-2}).$$

Pour que $(f_j)_\sigma(b)$ appartienne à \mathfrak{P}^{e_j+1} , il faut et il suffit que $x_0 + x_1 r^{e_j-1} + \dots + x_{q-2} (r^{e_j-1})^{q-2}$ appartienne à $p\mathbf{Z}_{(p)}$.

Considérons alors l'application $\mathbf{Z}_{(p)}$ -linéaire λ_j de $\mathbf{Z}_{(p)}[\theta]$ dans \mathbf{F}_p , définie par $\theta \mapsto \bar{r}^{e_j-1}$; (\bar{r} est la classe de r modulo p). Comme e_j est distinct de 1, \bar{r}^{e_j-1} est un élément d'ordre q de \mathbf{F}_p^* , et l'on vérifie facilement que λ_j est un homomorphisme d'anneaux surjectif. Son noyau est donc un idéal premier \mathfrak{p}_q de $\mathbf{Z}_{(p)}[\theta]$, au-dessus de p .

Comme tout sous-groupe de \mathbf{F}_p^* est cyclique, pour tout $e_k \neq 1$, il existe $x \in \mathbf{Z}$ tel que $\bar{r}^{e_k-1} = \bar{r}^{x(e_j-1)}$; l'application $\theta \mapsto \theta^x$ se prolonge en un automorphisme X de $\mathbf{Z}_{(p)}[\theta]$, et le diagramme suivant est commutatif :

$$\begin{array}{ccc} & X & \\ & \searrow & \rightarrow \mathbf{Z}_{(p)}[\theta] \\ \mathbf{Z}_{(p)}[\theta] & & \\ & \swarrow & \searrow \\ & \mathbf{F}_p & \end{array}$$

Les noyaux de λ_j et λ_k sont donc conjugués. Comme p est totalement décomposé dans $\mathbf{Z}_{(p)}[\theta]$, les noyaux sont distincts dès que X est non trivial, c'est-à-dire dès que e_j et e_k sont différents.

On obtient ainsi que le sous-groupe $M_{(p)}^{(\sigma)}$ de $M_{(p)}$ fixe par σ est isomorphe à $\mathfrak{p}_q^{(1)} \dots \mathfrak{p}_q^{(u)}$, les $\mathfrak{p}_q^{(i)}$ étant des idéaux premiers de $\mathbf{Z}_{(p)}[\theta]$ au-dessus de p , deux à deux distincts, et u étant égal au nombre d'indices e_j distincts. Pour aboutir au résultat annoncé, il suffit ensuite de remarquer que seule la classe de \mathfrak{b} est déterminée; donc on peut choisir l'idéal \mathfrak{b} premier à p . ■

PROPOSITION 2.3. — Notons u l'entier qui vaut 0 si E_K est isomorphe à $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j \oplus \mathfrak{b}$, et qui est égal au nombre d'exposants e_j distincts, pour $1 \leq j \leq \ell$, si E_K est isomorphe à

$$\left(\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j, \mathfrak{b} \right) \bigoplus_{j=\ell+1}^q \mathfrak{P}^{e_j} \alpha_j.$$

Alors l'indice $[E_K : N_{K/k} E_K]$ vaut p^{q-1-u} .

Démonstration. — Supposons que E_K soit isomorphe à une extension de \mathfrak{b} par $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$, définie à l'aide du cocycle $f \in Z^1(G, \text{Hom}_Z(\mathfrak{b}, \bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j))$. A l'élément u de E_K est associé le couple (α, β) , $\alpha \in \bigoplus_{j=1}^q \mathfrak{P}^{e_j}$ et $\beta \in \mathfrak{b}$. Donc $N_{K/k} u$ correspond à :

$$(1 + \sigma + \dots + \sigma^{p-1})(\alpha, \beta) = ((1 + \zeta + \dots + \zeta^{p-1})\alpha + (f_\sigma + \dots + f_{\sigma^{p-1}})\beta, p\beta).$$

Or, pour $i > 1$, on a :

$$f_{\sigma^i}(\beta) = (\sigma f_{\sigma^{i-1}} + f_\sigma)(\beta) = (1 + \zeta + \dots + \zeta^{i-1})f_\sigma(\beta).$$

Donc,

$$(f_\sigma + \dots + f_{\sigma^{p-1}})(\beta) = f_\sigma(\beta)[1 + (1 + \zeta) + \dots + (1 + \zeta + \dots + \zeta^{p-2})] = \frac{f_\sigma(p\beta)}{1 - \zeta}.$$

D'où $(1 + \sigma + \dots + \sigma^{p-1})(\alpha, \beta) = \left(\frac{f_\sigma(p\beta)}{1 - \zeta}, p\beta\right)$, et les $\mathbf{Z}[G]$ -modules $p\mathfrak{b}$ et $N_{K/k} E_K$ sont isomorphes.

La proposition 2.2 donne l'image de E_k par ce même isomorphisme. Comme p est totalement décomposé dans l'extension $\mathbf{Q}(\theta)/\mathbf{Q}$, le calcul de l'indice $[E_k : N_{K/k} E_K]$ est alors immédiat. ■

Remarque. — On a vérifié dans [11] que pour qu'une extension galoisienne totalement réelle Λ/\mathbf{Q} admette une unité de Minkowski, il faut que pour toute extension intermédiaire Λ' , l'application $N_{\Lambda/\Lambda'} : E_\Lambda \rightarrow E_{\Lambda'}$ soit surjective. Donc si une extension métacyclique K/\mathbf{Q} de degré pq admet une unité de Minkowski, E_K est $\mathbf{Z}[G]$ -isomorphe à l'un des modules suivants :

$$\left(\bigoplus_{\substack{j=0 \\ j \neq 1}}^{q-1} \mathfrak{P}^j \alpha_j, \mathfrak{b}\right) \oplus \mathfrak{P}^e \alpha, \text{ ou } \left(\bigoplus_{\substack{j=0 \\ j \neq 1}}^{q-1} \mathfrak{P}^j \alpha_j \oplus \mathfrak{P}^e \alpha, \mathfrak{b}\right), \text{ avec } e \neq 1.$$

2.3. Calcul de l'indice $a = [E_K : E_L E_{L\sigma} \dots E_{L\sigma^{q-1}} E_k]$.

PROPOSITION 2.4. — L'entier u étant défini à la proposition 2.3, et les \tilde{e}_i à la proposition 2.1, si E_K est isomorphe à une extension de \mathfrak{b} par $\bigoplus_{i=1}^q \mathfrak{P}^{e_i} \alpha_i$, on a : $a = p^{\sum_{i=1}^q (q\tilde{e}_i - e_i) + u}$.

Démonstration. — L'isomorphisme Φ , qui associe à E_K une extension de \mathfrak{b} par $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j$, transforme $E_L E_{L^\sigma} \dots E_{L^{\sigma^{q-1}}}$ en $\bigoplus_{j=1}^q \mathfrak{P}_1^{\tilde{e}_j} \alpha_j A$; (on le démontre en utilisant la proposition 2.1, et le fait que $\{1, \zeta, \dots, \zeta^{q-1}\}$ est une A_1 -base de A). Comme Φ transforme E_k en un sous-groupe de \mathfrak{b} déterminé à la proposition 2.2, on a :

$$a = \left[\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \alpha_j : \bigoplus_{j=1}^q \mathfrak{P}_1^{\tilde{e}_j} \alpha_j A \right] \times [\mathfrak{b} : \Phi(E_k)] \\ = \prod_{j=1}^q N_{\mathfrak{O}(p)/\mathfrak{O}}(\mathfrak{P}_1^{\tilde{e}_j} A \times \mathfrak{P}^{-e_j}) \times p^u. \quad \blacksquare$$

Remarquons que l'indice a ne peut être égal à 1 que lorsque E_K est $\mathbf{Z}[G]$ -isomorphe à un module de la forme $\bigoplus_{i=1}^q \alpha_i A \oplus \mathfrak{b}$. D'autre part, on retrouve dans ce cas particulier la valeur maximum obtenue par F. Halter-Koch dans [6], c'est-à-dire $p^{q(q-1)}$; cette valeur correspond au cas où E_K est isomorphe à $\bigoplus_{i=1}^q \mathfrak{P} \alpha_i \oplus \mathfrak{b}$, ou à $(\mathfrak{P}^2 \alpha_1, \mathfrak{b}) \bigoplus_{i=2}^q \mathfrak{P} \alpha_i$; si l'on modifie l'un des e_i , l'exposant de p diminue d'au moins une unité dans $\left[\bigoplus_{i=1}^q \mathfrak{P}^{e_i} \alpha_i : \bigoplus_{i=1}^q \mathfrak{P}_1^{\tilde{e}_i} \alpha_i A \right]$, et augmente d'au plus une unité dans $[\mathfrak{b} : \Phi(E_k)]$.

Pour tout corps de nombres Λ , désignons par h_Λ son nombre de classes d'idéaux. L'indice a est apparu dans le calcul du rapport $\frac{h_K}{h_k \cdot h_L^q}$, effectué dans [6]; on démontre en effet que $\frac{h_K}{h_k \cdot h_L^q} = \frac{a}{p^{\frac{(q-1)(q+2)}{2}}}$. A l'aide des notations des propositions 2.1 et 2.3, on obtient :

$$\frac{h_K}{h_k \cdot h_L^q} = p^{\sum_{i=1}^q (q\tilde{e}_i - e_i) + u - \frac{(q-1)(q+2)}{2}}.$$

2.4. Invariant de Brauer-Walter.

Soit Γ un groupe fini, et Δ un sous-groupe de Γ . Si M est un Γ -module, désignons par M^Δ le sous-groupe de M fixe par Δ . C.D. Walter étudie dans [17] les Γ -modules de caractère donné; il démontre en particulier que si l'on a une relation de dépendance

linéaire, à coefficients dans \mathbf{Z} , de caractères induits, $\sum_{\Delta} a_{\Delta} \chi_{\Delta}^* = 0$, et si les modules M et N sont $\mathbf{Z}[\Gamma]$ -isomorphes, alors $\prod_{\Delta} [M^{\Delta} : N^{\Delta}]^{a_{\Delta}} = 1$.

DEFINITION. — Soit Γ un groupe fini, M et N deux $\mathbf{Z}[\Gamma]$ -modules de même caractère, et $\mathcal{R} : \sum_{\Delta} a_{\Delta} \chi_{\Delta}^* = 0$ une relation de dépendance linéaire non triviale, à coefficients dans \mathbf{Z} , de caractères induits. On appelle invariant de Brauer-Walter associé à la relation \mathcal{R} et aux modules M et N le produit $J_{\mathcal{R}}(M, N) = \prod_{\Delta} [M^{\Delta} : N^{\Delta}]^{a_{\Delta}}$.

On pourra trouver dans un exposé de J.J. Payan [12] quelques propriétés et quelques exemples d'utilisation de cet invariant. En particulier J.J. Payan démontre que si pour tout nombre premier ℓ , les localisés $\mathbf{Z}_{(\ell)} \otimes M$ et $\mathbf{Z}_{(\ell)} \otimes N$ sont $\mathbf{Z}_{(\ell)}[\Gamma]$ -isomorphes, $J_{\mathcal{R}}(M, N) = 1$.

D'après un théorème classique de R. Brauer [1], pour un groupe métacyclique d'ordre pq , toutes les relations non triviales entre caractères induits sont des conséquences de la relation \mathcal{R} :

$$q\chi_G - \chi_H^* + \chi_{\{1\}}^* - q\chi_g^* = 0.$$

Comme représentants des $\mathbf{Z}[G]$ -modules de caractère $\chi_{\{1\}}^* - \chi_G$, modulo l'isomorphisme des localisés en ℓ pour tout nombre premier ℓ , choisissons les modules de la forme $\left(\bigoplus_{j=1}^s \mathfrak{P}^{e_j}, B \right) \bigoplus_{j=s+1}^q \mathfrak{P}^{e_j}$ ou $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \oplus B$. Toutes les valeurs de $J_{\mathcal{R}}(M, N)$ s'obtiennent à l'aide du résultat suivant :

PROPOSITION 2.5. — Posons $T = A^q \oplus B$. Pour chacun des $\mathbf{Z}[G]$ -modules ci-dessus, $J_{\mathcal{R}}(M, T) = a$, où a est l'indice associé à M calculé dans la proposition 2.4.

Démonstration. — Si M est de la forme $\bigoplus_{j=1}^q \mathfrak{P}^{e_j} \oplus B$, M est contenu dans T , et le calcul de $J_{\mathcal{R}}(M, T)$ est immédiat.

Si M s'écrit $\left(\bigoplus_{j=1}^s \mathfrak{P}^{e_j}, B \right) \bigoplus_{j=s+1}^q \mathfrak{P}^{e_j}$, notons M_1 le sous-groupe de $\left(\bigoplus_{j=1}^s \mathfrak{P}^{e_j}, B \right)$ fixe par σ . On vérifie facilement que $(pA)^q \oplus M_1$ est un sous- $\mathbf{Z}[G]$ -module de M isomorphe à T ; d'où le calcul de $J_{\mathcal{R}}(M, T)$. ■

Lorsque K admet une unité de Minkowski, E_K est $\mathbf{Z}[G]$ -isomorphe au module $M = \mathbf{Z}[G]/\mathbf{Z}\tilde{G}$, où \tilde{G} désigne l'élément $\sum_{\sigma \in G} \sigma$ de $\mathbf{Z}[G]$. En utilisant la remarque du paragraphe 2.2, on obtient : $J_{\mathfrak{R}}(M, T) = \frac{1}{2} q^{(q-1)+q\tilde{e}-e}$. La connaissance de cet invariant équivaut à celle de l'indice e . Si $e = 1$, ou bien si le groupe $\langle U^*, V^* \rangle$ défini dans la proposition 1.4 est identique à $(\mathbf{Z}/p\mathbf{Z})^*$, on connaît la structure de M modulo les $\mathbf{Z}_{(\ell)}[G]$ -isomorphismes, pour tout nombre premier ℓ . Nous effectuerons le calcul de $J_{\mathfrak{R}}(M, T)$ dans un cas particulier, au paragraphe 4.

3. CONTRAINTES GALOISIENNES SUR LE GROUPE DES CLASSES D'IDEAUX DE K

Lorsqu'on connaît la structure de G -module de E_K , on détermine assez facilement les groupes $H^n(H, U_K)$ et $H^n(g, U_K)$. Or d'après K. Iwasawa [7], ces groupes s'interprètent en termes d'idéaux ou de classes d'idéaux. En particulier, K. Iwasawa démontre :

PROPOSITION 3.1. — *Soit Λ'/Λ une extension galoisienne finie de corps de nombres, de groupe de Galois Γ . Le groupe $H^1(\Gamma, U_{\Lambda'})$ est canoniquement isomorphe au quotient du groupe des idéaux principaux invariants de Λ' modulo le groupe des idéaux principaux de Λ .*

L'interprétation du deuxième groupe de cohomologie est moins simple. Dans l'article de K. Iwasawa, on trouve encore :

PROPOSITION 3.2. — *Si Λ'/Λ est non ramifiée, $H^2(\Gamma, U_{\Lambda'})$ est isomorphe au quotient du groupe des classes invariantes de Λ'/Λ par le groupe des classes représentées par des idéaux de Λ .*

Reprenons les calculs dans le cas où il y a ramification. Si l'on désigne par :

- I_K le groupe des idéaux de K ,
- H_K le groupe des classes d'idéaux de K ,
- J_K le groupe des idèles de K ,

C_K le groupe des classes d'idèles de K ,
 P_K le groupe des idèles principaux de K ,
 W_K le noyau de l'homomorphisme canonique de J_K sur I_K ,

on a des isomorphismes bien connus entre les groupes suivants :
 $P_K \cap W_K$ et I_K , $J_K/P_K W_K$ et H_K , P_K/U_K et $P_K W_K/W_K$, et
 $P_K W_K/P_K$ et W_K/U_K . Donc la suite exacte :

$$1 \longrightarrow P_K W_K/W_K \longrightarrow J_K/P_K \longrightarrow J_K/P_K W_K \longrightarrow 1$$

s'écrit aussi :

$$1 \longrightarrow W_K/U_K \longrightarrow C_K \longrightarrow H_K \longrightarrow 1.$$

Comme K/\mathbf{Q} est une extension galoisienne de groupe G , la suite exacte ci-dessus est une suite de Δ -modules, pour tout sous-groupe Δ de G , et l'on peut écrire la suite de cohomologie associée au groupe Δ . Or, d'après un théorème de J. Tate (qui figure par exemple dans [2], p. 197), le groupe $\hat{H}^i(\Delta, C_K)$ est isomorphe à $\hat{H}^{i-2}(\Delta, \mathbf{Z})$, où Δ agit trivialement sur \mathbf{Z} . Si Δ est cyclique d'ordre α , pour i impair, $\hat{H}^i(\Delta, C_K)$ est trivial, et pour i pair, $\hat{H}^i(\Delta, C_K)$ est isomorphe à $\mathbf{Z}/\alpha\mathbf{Z}$. Dans ce cas, on a la suite exacte (1) :

$$0 \longrightarrow H^1(\Delta, H_K) \longrightarrow H^2(\Delta, W_K/U_K) \longrightarrow \mathbf{Z}/\alpha\mathbf{Z} \longrightarrow H^2(\Delta, H_K) \\ \longrightarrow H^3(\Delta, W_K/U_K) \longrightarrow 0.$$

La détermination des groupes $H^i(\Delta, W_K/U_K)$ s'effectue à partir des groupes de cohomologie de U_K et W_K .

PROPOSITION 3.3. — Soit K/\mathbf{Q} une extension métacyclique de degré pq . L'entier u étant défini dans la proposition 2.3, on a :

$$H^1(H, U_K) \simeq \mathbf{F}_p^{q-u}, \quad H^2(H, U_K) \simeq \mathbf{F}_p^{q-1-u} \\ H^1(g, U_K) \simeq \mathbf{F}_q \quad \text{et} \quad H^2(g, U_K) = (0).$$

Démonstration. — Remarquons que U_K et E_K admettent mêmes groupes de cohomologie relativement à H et à g . En effet, on a la suite exacte :

$$1 \longrightarrow \{\pm 1\} \longrightarrow U_K \longrightarrow E_K \longrightarrow 1;$$

comme les groupes H et g sont d'ordre impair, les groupes de cohomologie de $\{\pm 1\}$ sont triviaux.

Le calcul des groupes $H^2(g, E_K)$ et $H^2(H, E_K)$ est immédiat grâce aux propositions 2.1 et 2.3. Comme on connaît les quotients de Herbrand (voir H. Yokoi [19], lemme 3), on en déduit les groupes $H^1(g, E_K)$ et $H^1(H, E_K)$. ■

Remarque. — D'après C.D. Walter [18], l'homomorphisme "d'extension" est une injection du groupe des classes de L dans le groupe des classes de K . Comme $H^1(g, U_K)$ n'est jamais trivial, d'après la proposition 3.1, K possède un idéal principal produit de puissances d'idéaux premiers ramifiés dans K/L .

Choisissons pour Δ le sous-groupe g , et notons t le nombre d'idéaux premiers ramifiés dans K/L . D'après la théorie du corps de classes local, on a : $H^1(g, W_K) \simeq H^2(g, W_K) \simeq \mathbf{F}_q^t$. Donc, en utilisant la proposition 3.3, on obtient que $H^2(g, W_K/U_K)$ est un \mathbf{F}_q -espace vectoriel de dimension t ou $t+1$. Et grâce à la suite exacte (1), on vérifie que les deux \mathbf{F}_q -espaces vectoriels $H^1(g, H_K)$ et $H^2(g, H_K)$ sont isomorphes de dimension $t-1$, t ou $t+1$. Rappelons que $H^2(g, H_K)$ s'interprète comme quotient du groupe des classes invariantes relatives à K/L par le groupe $N_{K/L} H_K$; quant à $H^1(g, H_K)$, il est isomorphe au quotient du groupe des classes de norme triviale sur L par le sous-groupe des classes quotients d'une classe de K par sa conjuguée par τ . Ces résultats fournissent en particulier une minoration du q -rang du groupe des classes de K invariantes par g , à rapprocher de celle donnée par J. Martinet [10 bis].

Si l'on remplace g par H , et si l'on note t' le nombre d'idéaux premiers ramifiés dans K/k , on a encore :

$$H^1(H, W_K) \simeq H^2(H, W_K) \simeq \mathbf{F}_p^{t'}.$$

Comme les groupes $H^i(H, U_K)$ sont moins simples que les groupes $H^i(g, U_K)$, nous ne ferons pas d'étude générale de ce cas.

4. EXEMPLES NUMERIQUES

Citons d'abord quelques résultats de la théorie du corps de classes global, qui assurent l'existence de telles extensions.

THEOREME 4.1. — Soit k/\mathbf{Q} une extension cyclique de degré q premier, et soit p un nombre premier congru à 1 modulo q . Si p divise le nombre de classes d'idéaux de k , il existe des extensions K cycliques non ramifiées de k , de degré p sur k , et galoisiennes non abéliennes sur \mathbf{Q} .

Ce théorème figure par exemple dans [3]. D'autre part, H. Kisilevsky a démontré dans [8] le résultat suivant :

THEOREME 4.2. — Si Λ est un corps de nombres dont le p -groupe des classes est cyclique d'ordre p , la p -tour des corps de classes est de longueur 1.

Enfin l'on a (cf. [19]) :

THEOREME 4.3. — Soit Λ' une extension cyclique non ramifiée d'un corps de nombres Λ . Si le nombre de classes d'idéaux de Λ qui deviennent principales dans Λ' est égal à $[\Lambda' : \Lambda]$, alors : $U_{\Lambda} = N_{\Lambda'/\Lambda} U_{\Lambda'}$.

Lorsqu'on parcourt la table figurant dans l'article [5], on remarque des corps cubiques cycliques à nombre de classes premier congru à 1 modulo 3. Le premier rencontré est le corps k de discriminant 313^2 , de nombre de classes 7 ; il existe donc une extension K/k non ramifiée, telle que K/\mathbf{Q} soit métacyclique de degré 21. D'après les théorèmes 4.2 et 4.3 le nombre de classes de K n'est pas divisible par 7, et l'application $N_{K/k} : U_K \longrightarrow U_k$ est surjective.

Compte-tenu des résultats des paragraphes 1.4 et 2.2, et du fait que les corps cyclotomiques $\mathbf{Q}^{(7)}$ et $\mathbf{Q}^{(3)}$ sont principaux, E_K est $\mathbf{Z}[G]$ -isomorphe à un module du type : $(A \oplus \mathfrak{P}^2, B) \oplus \mathfrak{P}^e$. (Pour $p = 7$ et $q = 3$, on peut en effet utiliser les lemmes 1.5 et 1.6). D'après la proposition 2.4, l'indice $a = [E_K : E_L E_{L\sigma} E_{L\sigma^2} E_k]$ vaut $7^{3+3\tilde{e}-e}$, l'entier \tilde{e} étant égal à 0 pour $e = 0$, et à 1 sinon. La formule du nombre de classes, rappelée au paragraphe 2.3, conduit à l'égalité : $h_K = 7^{3\tilde{e}-e-1} \times h_L^3$. Comme 7 ne doit pas diviser h_K , nécessairement h_L est premier à 7, et e vaut 2 ; ainsi la structure de $\mathbf{Z}[G]$ -module de E_K est parfaitement déterminée : E_K est $\mathbf{Z}[G]$ -isomorphe à $(A \oplus \mathfrak{P}^2, B) \oplus \mathfrak{P}^2$.

Comme l'application $N_{K/k} : E_K \longrightarrow E_k$ est surjective, on peut se poser la question de savoir si K admet une unité de Minkowski. Le lemme suivant prouve qu'il n'en est rien.

LEMME 4.4. — Soit K une extension métacyclique de \mathbf{Q} , de degré 21. Si K admet une unité de Minkowski, E_K est $\mathbf{Z}[G]$ -isomorphe au module $(A \oplus \mathfrak{F}^2, B) \oplus \mathfrak{F}$.

Démonstration. — Posons encore $M = \mathbf{Z}[G]/\mathbf{Z}\tilde{G}$, avec $\tilde{G} = \sum_{\sigma \in G} \sigma$. D'après la dernière remarque du paragraphe 2, la structure de $\mathbf{Z}[G]$ -module de M est connue sans ambiguïté si l'on sait calculer l'invariant $J_R(M, T) = a$ associé.

Tout élément de M s'écrit de manière unique :

$$\alpha = \sum_{i=0}^6 (\lambda_i + \mu_i \tau + \nu_i \tau^2) \sigma^i, \quad \text{avec} \quad \sum_{i=0}^6 (\lambda_i + \mu_i + \nu_i) = 0.$$

On vérifie facilement que pour que α soit fixe par τ (resp. $\tau\sigma$, resp. $\tau\sigma^2$, resp. σ), il doit s'écrire :

$$\begin{aligned} \alpha &= (1 + \tau + \tau^2) \sum a_i \sigma^i && \text{avec} \quad \sum a_i = 0, \\ \text{resp. } \alpha &= (1 + \tau\sigma + (\tau\sigma)^2) \sum b_i \sigma^i && \text{avec} \quad \sum b_i = 0, \\ \text{resp. } \alpha &= (1 + \tau\sigma^2 + (\tau\sigma^2)^2) \sum c_i \sigma^i && \text{avec} \quad \sum c_i = 0, \\ \text{resp. } \alpha &= (\lambda + \mu\tau + \nu\tau^2) \sum \sigma^i && \text{avec} \quad \lambda + \mu + \nu = 0. \end{aligned}$$

Etant donné λ_i, μ_i, ν_i , cherchons à quelles conditions l'on peut trouver $\lambda, \mu, \nu, a_i, b_i$ et c_i tels que :

$$\begin{aligned} \sum (\lambda_i + \mu_i \tau + \nu_i \tau^2) \sigma^i &= (1 + \tau + \tau^2) \sum a_i \sigma^i \\ &+ (1 + \tau\sigma + (\tau\sigma)^2) \sum b_i \sigma^i + (1 + \tau\sigma^2 + (\tau\sigma^2)^2) \sum c_i \sigma^i \\ &+ (\lambda + \mu\tau + \nu\tau^2) \sum \sigma^i. \end{aligned}$$

Il est clair qu'il faut d'abord que $\sum \lambda_i \equiv \sum \mu_i \equiv 0(7)$. Ces conditions étant réalisées, les valeurs de λ, μ, ν sont déterminées ; posons alors $\lambda'_i = \lambda_i - \lambda$, $\mu'_i = \mu_i - \mu$ et $\nu'_i = \nu_i - \nu$. Comme $\tau\sigma = \sigma^2\tau$, $\sigma\tau = \tau\sigma^4$, et l'on obtient le système suivant, où les indices sont définis modulo 7 :

$$\begin{cases} \lambda'_i = a_i + b_i + c_i \\ \mu'_i = a_i + b_{i-1} + c_{i-2} \\ \nu'_i = a_i + b_{i-5} + c_{i-3} \end{cases} \quad (1)$$

D'où :

$$\begin{cases} \varrho_i = \mu'_i - \lambda'_i = b_{i-1} - b_i + c_{i-2} - c_i \\ m_i = \nu'_i - \lambda'_i = b_{i-5} - b_i + c_{i-3} - c_i. \end{cases} \quad (2)$$

En éliminant les b_i , il vient :

$$\varrho_{i+1} + \varrho_{i+2} + m_i = c_{i+4} + c_{i-1} - c_{i+1} - c_{i+2}. \quad (3)$$

Posons $d_i = c_{i+2} - c_i$. Le système (3) se transforme en :

$$\varrho_{i+1} + \varrho_{i+2} + m_i = d_{i+2} - d_{i-1}. \quad (4)$$

Comme $\sum \varrho_i = \sum m_i = 0$, la septième équation du système est une conséquence des autres ; les six premières équations permettent de calculer tous les d_i en fonction de d_0 . Le choix de d_0 est imposé par la condition $\sum d_i = 0$, qui s'exprime encore : $7d_0 + F_1(\lambda_i, \mu_i, \nu_i) = 0$, où F_1 est une forme linéaire à coefficients dans \mathbf{Z} . Le calcul de d_0 n'est possible que si $F_1(\lambda_i, \mu_i, \nu_i) \equiv 0 \pmod{7}$; remarquons que cette condition n'est pas triviale, puisque ν_i n'y intervient que par l'intermédiaire de l'expression : $6m_1 + 5m_4 + 4m_0 + 3m_3 + 2m_6 + m_2$.

Les d_i étant ainsi obtenus, six des formules de définition des d_i donnent les c_i en fonction de c_0 , tandis que la septième est une conséquence des autres. Comme on doit avoir $\sum c_i = 0$, c_0 vérifie l'égalité : $7c_0 + 7 \times 3d_0 + F_2(\lambda_i, \mu_i, \nu_i) = 0$, F_2 étant une forme linéaire à coefficients dans \mathbf{Z} . D'où une nouvelle condition : $F_2(\lambda_i, \mu_i, \nu_i) \equiv 0 \pmod{7}$, indépendante de la précédente, puisque les ν_i figurent uniquement dans l'expression : $m_1 + 4m_0 + 6m_3 + 6m_6 + 4m_2$.

On utilise alors les six premières équations du système (2), qui définissent tous les b_i en fonction de b_0 ; exprimer que $\sum b_i = 0$ conduit à imposer une nouvelle condition, $F_3(\lambda_i, \mu_i, \nu_i) \equiv 0 \pmod{7}$, où les ν_i interviennent par : $2m_1 + m_0 + 5m_3 + 5m_6 + m_2$. On obtient sans problème les a_i à partir de (1). L'indice a cherché vaut donc 7^5 , et $e = 1$. ■

Pour terminer l'étude de ce cas particulier, voyons ce que l'on peut obtenir du calcul des groupes de cohomologie de U_K et H_K . Les résultats relatifs au sous-groupe H sont déjà exploités : ils se retrouvent dans la théorie du corps de classes.

Pour le sous-groupe g , la proposition 3.3 donne :

$$H^1(g, U_K) \simeq \mathbf{F}_3 \quad \text{et} \quad H^2(g, U_K) = (0).$$

D'après [12], il existe dans K/L un unique idéal premier ramifié, qui est au-dessus de 313 ; comme C.D. Walter a montré dans [18] l'injectivité de l'homomorphisme d'extension des idéaux, $j_{K/L} : H_L \longrightarrow H_K$, on déduit de la proposition 3.1 que tout idéal premier de K au-dessus de 313 est équivalent à l'étendu d'un idéal de L ou d'un de ses conjugués. Remarquons de plus que le groupe des classes invariantes par g est isomorphe à H_L ; donc le 3-rang du groupe H_L est supérieur ou égal à la dimension du \mathbf{F}_3 -espace vectoriel $H^2(g, H_K)$. En particulier, si 3 ne divise pas h_L , toute classe de K de norme triviale sur L est quotient d'une classe de K par sa conjuguée par τ .

Comme la table [5] fournit aussi des corps cubiques cycliques de nombre de classes 13 ou 19, on pourrait construire de manière analogue des extensions métacycliques de degré 3×13 ou 3×19 , non ramifiées dans la branche K/k . Remarquons enfin qu'il serait possible de préciser numériquement les corps ainsi définis : J. Cougnard indique en effet dans [3] une méthode pour déterminer le polynôme irréductible d'un élément primitif de K .

BIBLIOGRAPHIE

- [1] R. BRAUER, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpers, *Math. Nachr.*, 4 (1951), 158-174.
- [2] J. CASSELS et A. FRÖHLICH, Algebraic Number Theory. Academic Press, New-York, 1967.
- [3] J. COUGNARD, Sur les extensions galoisiennes non abéliennes de degré pq du corps des rationnels (p et q premiers), thèse de 3^e cycle, Bordeaux, 1972.
- [4] S. GALOVITCH, I. REINER et S. ULLOM, Class groups for integral representations of metacyclic groups, *Mathematika*, 19 (1972), 105-111.

- [5] M.N. GRAS, N. MOSER et J.J. PAYAN, Approximation algorithmique du groupe des classes de certains corps cubiques cycliques, *Acta Arithmetica*, 23 (1973), 295-300.
- [6] F. HALTER-KOCH et N. MOSER, Sur le nombre de classes de certaines extensions métacycliques sur \mathbf{Q} ou sur un corps quadratique imaginaire, *J. Math. Soc. Japan*, 30 (1978), 237-248.
- [7] K. IWASAWA, A note on the group of units of an algebraic number field, *J. Math. pures et appliquées*, 35 (1956), 189-192.
- [8] H. KISILEVSKY, Some results related to Hilbert's theorem 94, *J. Number Theory*, 2 (1970), 198-206.
- [9] S.N. KURODA, Über die Klassenzahl eines relativ zyklischen Zahlkörpers von Primzahlgrade, *Proc. Japan Academy*, 40 (1964), 623-626.
- [10] LENA CHANG PU, Integral representations of non abelian groups of order pq , *Mich. Math. J.*, 12 (1965), 231-246.
- [10bis] J. MARTINET, Tours de corps de classes et estimations de discriminants, *Inventiones math.*, 44 (1978), 65-73.
- [11] N. MOSER, Unités et nombre de classes d'une extension galoisienne diédrale de \mathbf{Q} , *Abh. Math. Sem. Hamburg* (à paraître).
- [12] J.J. PAYAN, Sur le théorème des indices de Brauer-Walter. Application à l'existence d'unités de Minkowski, *Sém. Th. Nb.*, Grenoble, 1975-1977.
- [13] J. PORUSCH, Die Arithmetik in Zahlkörpern, deren zugehörige Galoische Körper spezielle metabelsche gruppen besitzen, auf klassenkörpertheoretischer Grundlage, *Math. Z.*, 37 (1933), 134-160.
- [14] I. REINER et C. CURTIS, Representation theory of finite groups and associative algebras, Interscience New-York, 1962.
- [15] M. ROSEN, Representations of twisted group rings, Ph. D. Thesis, Princeton, 1963.
- [16] Représentations entières de certains groupes finis, *Sém. Th. Nb.*, Grenoble, 1973-1974.
- [17] C.D. WALTER, Brauer class number relation. (à paraître dans *Acta Arithmetica*).

- [18] C.D. WALTER, A class number relation in Frobenius extensions of number fields, *Mathematika*, 24 (1977), 216-225.
- [19] H. YOKOI, On the class number of a relatively cyclic number field, *Nagoya Math. J.*, 29 (1967), 31-44.

Manuscrit reçu le 28 avril 1978.

Nicole MOSER,
Université de Grenoble I
Laboratoire de Mathématiques Pures
Associé au CNRS
Institut Fourier
B.P. 116
38402 St Martin d'Hères.